IT Procurement: Time for Change

General Assembly of the State of Tennessee
Fiscal Review Committee
October 21, 2014

Dugan Petty
Senior Fellow
Center for Digital Government
Governing Institute

A national research and advisory institute on information technology policies and best practices in state and local government

www.centerdigitalgov.com

Procurement Rules

Intended to protect the public's interest: missing the mark in IT

- IT - dynamic evolution (XaaS, Cloud, Mobile, Security)

- Procurement Practices – reactive, borrowed, mismatched with problems to be solved in today's digital environment

- Failed IT Procurements and Contracts - create distrust and lack of credibility with the public

- Agency Concerns - takes too long and don't get the results

- Suppliers Perception - unresponsive, overly rigid, drawn out and high risk

Key Trouble Spots

Requirements - high risk on a good day when everyone is engaged

- Understand the business objectives – high end-user involvement

- Avoid large high risk projects

- Agile development, incremental contracting, pilot & test drive solutions lower risk and get better results

Key Trouble Spots

Rigid Ineffective Processes – not getting results

- Use more discussions and negotiations in RFP – best fit saves time and money over cheapest price

- Use acquisition models designed to deliver the project results (Best Value, Incentives, Requests for Demonstration, Multiple Rounds, Modular Contracting, Accelerators)

- Simplify processes – apply quality management. Include providers and stakeholders

- Improve vendor performance through evaluation, prequalification and award criteria

Key Trouble Spots

Communication Barriers– disrupts partnerships between providers and public jurisdictions, increases potential for protests

- Build in effective and appropriate communication at every phase of procurement and contract execution – end to end review

- Regular vendor/provider forums

- Debrief vendors after award

- Better communication and effective protest rules reduce protests

Key Trouble Spots

Terms and Conditions – often disconnected from reasonable commercial contract practices

Review and revise to commercially reasonable - CA and OR

Must fit the state's need, risk profile and the provider's business model, one size does not fit all

New IT driven technologies are creating new business models - need new control models

Key Trouble Spots

Functional separation (Silos) – projects fail when the project is tossed over the wall to be procured

- Integrated Project Team

- Contract Management Office - CA Office of System Integration Model

- Match control with authority and resources

Risk Adverse Culture – does not lead to improvement & stifles innovation

- Measure results, evaluate practice, lean the process, encourage innovation, sharing, & collaboration

7 Steps to Improvement

1. Create flexibility – use discussions &negotiations, performance based, best value, incentives, multiple rounds of negotiations, modular contracts, and Requests for Demonstration (RFD)

2. Evaluate, use and refine alternative contracting models – ABA Special Procurement

3. Modernize IT T&Cs to commercially reasonable and realistic standards for your specific business needs in collaboration with industry trade groups and other states

4. Improve provider and state official communication at all levels of procurement and contracting. Create discussion forums with providers for new ideas

5. Incent better provider and vendor performance – eliminate barriers to getting the A team, evaluate vendor performance

6. Participate in cooperative procurements with other states and jurisdictions

7. Foster an environment to innovate, incubate and collaborate

CLOUD AND AS-A-SERVICE PROCUREMENTS

Model Terms and Conditions - SaaS, PaaS & IaaS

Guiding Principles

Procurement Approach

Lessons Shared

---

21 Steps *to the* Cloud

These best practices will help you arrive at better service contracts!

The Center for Digital Government's *Guide to Cloud Procurements* includes 21 model contract terms developed by a team of 12 governments and 14 companies — all designed to help public agencies buy software, infrastructure and platforms as a service. The guide, available at **govtech.com/procurement**, provides nearly 80 pages of pure procurement satisfaction. 21 Steps to the Cloud to gives you a taste of what's inside.

Data

Governments have a fundamental responsibility to limit access to non-public data and protect data integrity. These steps cover data ownership and management concerns.

WELCOME TO THE CLOUD!

END

Protect sensitive data by requiring encryption.

Define provider data access narrowly — just enough to deliver the service.

Identify data roles and responsibilities, but remember that you own the data.

Insist that providers use only U.S. data centers — but let tech support "follow the sun."

Affirm your right to import and export data whenever you need to.

Breach Notification

Prompt notice of a security incident gives agencies time to take appropriate action. Defining provider liability for a data breach can be difficult. These steps can help.

Make sure your cloud company tells you about e-discovery or other legal requests.

Agree on a format and timeframe for providers to return your data if a service terminates.

Cap provider liability for data breaches — use a set amount per record or per person.

Few providers will agree to unlimited liability for security breaches. If your contract demands it, you'll have trouble attracting bidders.

Require providers to notify you of unauthorized data theft or disclosure within 24 hours, or sooner if required by state law.

Make sure cloud companies perform background checks on employees and subcontractors.

Software as a Service
Service provider owns and operates all software and hardware needed to provide the service.

Require your provider to disclose non-proprietary security processes.

Infrastructure as a Service
Hosted processing, storage and network resources that can be quickly provisioned to run your own applications.

Insist on separation of job duties for provider staff; require reasonable nondisclosure.

Classify your data by security category, then match your cloud provider's security to the data classifications.

Providers will struggle to estimate their costs if they don't have a clear understanding of the appropriate level of control and security for your data.

Establish your right to remove contractor staff and spell out the conditions for doing so.

Personnel
Public jurisdictions must guard their data no matter where it is. Protect yourself from internal data security threats by following these steps.

Security
You'll need to perform due diligence on your service provider's security practices. These steps will help ensure your data is safe.

Demand access to provider security logs and reports; spell out reporting formats in an SLA.

Specifying traditional auditing practices in your contract can be a barrier to acquiring services.

Audit your cloud company to ensure it's conforming with the contract.

Providers shouldn't store sensitive data on mobile devices; if data has to be mobile, make sure it's encrypted at rest.

Require your cloud provider to perform independent audits of its data centers annually.

Audits
Oversight and control are critical for any public expenditure. These steps will help you tailor audits to fit the service model.

Platform as a Service
Hosted infrastructure where you can create or acquire applications using tools and programming languages supported by the service provider.

START

Make sure you get advance notice of upgrades or system changes.

Require disclosure of all subcontractors and business partners involved with your apps and data.

Insist on a detailed business continuity and disaster recovery plan from your provider.

Operations
Use these steps to assure that your cloud provider's

CENTER FOR DIGITAL

Reference Material

- Transforming Procurement For the 21st Century: Part 1: Reforming IT Terms and Conditions to Improve Procurement Environments and Outcomes , TechAmerica, March, 2009

- Gaining Traction on the road to win-win: Limitations on liability in state IT contracting, NASCIO, 2010

- "Myth-Busting": Addressing Misconceptions to Improve Communications with Industry during the Acquisition Process, Daniel I. Gordon, February 2, 2011, OMB

- "Myth-Busting 2", Addressing Misconceptions and Further Improving Communications During the Acquisition Process, Lesley A. Field, May 7, 2012, OMB

- Enterprise Risk Management for Cloud Computing, Committee of Sponsoring Organizations of the Treadway Commission, June 2012

- Leveraging Enterprise Architecture for Improved IT Procurement, July 2012, NASCIO

- Leaving Performance Bonds at the Door for Improved IT Procurement, NASCIO, August 2012

- Recommendations to Improve Large Information Technology Procurements: A Road Map for Success in California, CA Task Force on Reengineering IT Procurement for Success, August 2013

- Seeing Excellence: Learning from Great Procurement Teams, Richard Pennington, 2013

- Strategies For Procurement Innovation and Reform, IJIS Institute, December 2013

- Best Practice Guide For Cloud and As-A-Service Procurements, Center for Digital Government, September 10, 2014

Questions & Answers